REMARKS

Reconsideration of the above-identified application in view of the amendments above and the following remarks is respectfully requested. No new material has been entered.

Specification

The Examiner has objected to the abstract as being longer than the allowed 150 words. In accordance with the Examiner's objection, a new abstract has been submitted for substitution, to fall within the allowed word count.

Claims

Claims 1 – 28 are in this case.

- The Examiner has rejected claims 13, 14, 16, and 20 under 35 USC §112, second paragraph, as being indefinite.
- The Examiner has further rejected claims 1 - 7, 10 - 15, 17, 21, 23, 24, and 28 under 35 USC §102(b) as being anticipated by Moskowitz et al. (U.S. 5,745,569).
- The Examiner has moreover rejected claims 8, 9, 16, 18 - 20, 22, and 25 - 27 under 35 USC §103(a) as being unpatentable over Moskowitz et al. in view of various other prior art as cited in the Office Action.

The above rejections of claims 1 - 3, 6, 7, 11, 21, and 28 according to 35 USC §102 (b), however, are respectfully traversed, as set forth in detail below.

§112 Rejections

The Examiner has rejected claims 13, 14, 16, and 20 under 35 USC §112, second paragraph, as being indefinite, and has provided clarifying details as to the basis for this rejection.

Having taken careful note of the points raised by the Examiner, the Applicant respectfully submits that the above amendments to claims 13, 14, and 16 serve to remove the indefiniteness cited by the Examiner, and thereby render the subject claims to be in compliance with 35 USC §112. The Applicant further notes that claim 20 was rejected by the Examiner under 35 USC §112 because of its dependency on claim 16, and that with the above current amendment to claim 16, the Applicant respectfully submits that claim 20 is also now in compliance with 35 USC §112.

§102(b) Rejections

The §102(b) rejections of claims 1 - 3, 6, 7, 11, 21, and 28 as being anticipated by Moskowitz, et al., are respectfully traversed, as set forth below:

General Discussion of U.S. 5,745,569 to Moskowitz, et al.

Moskowitz, et al. discloses a method of protecting a computer program from unauthorized distribution by hiding ("encoding") critical software code via a watermark within the digital resources (e.g., text, graphics, animations, sounds, etc.) of a computer program, such that a separate external key is necessary[1] to extract the critical code-

1. Moskowitz — (abstract): "A method for protecting computer code copyrights by encoding the code into a data resource with a digital watermark."; (col. 3, lines 13 - 18): "this invention ... focuses on watermarking with 'keys' derived from license codes or other ownership identification information, and using the watermarks encoded with such keys to hide an essential subset of the application code resources."

containing watermark and thereby allow the program to access the critical code.[2] If the user does not have the key, the program cannot operate.[3] According to Moskowitz, therefore, the key must accompany the program in order to use the program.[4]

Moreover, Moskowitz teaches that the key may be mathematically-derived from information about the computer program license.[5] This means that, according to Moskowitz, the licensing information (contained in the key) must always accompany the program — for otherwise, the program cannot function. Because of this, the program cannot be separated from its license by a user without becoming inoperative.

It is this binding of the program to the key which is the basis by which Moskowitz attempts to protect the program against unauthorized distribution. Moskowitz also optionally allows (but does not require) license information to contain personal information about the authorized user.[6] In this case, if the program is to remain operative, it cannot be separated from information about the authorized user that is contained in the key. Moskowitz also implies that the licensing information can be recovered from the key,[7] in which case the personal information about the authorized user (in the key) must accompany copies of the program if those copies are to be functional (Moskowitz, however, fails to

---

2. Moskowitz — (col. 5, lines 58 - 60): "For the encoding of the essential code resources, a 'key' is needed."; (col. 6, lines 6 - 7): "The key is necessary to access the underlying code..."

3. Moskowitz — (col. 5, lines 48 - 51): "...essential code resources are not stored in their own partition, but rather stored as encoded information in data resources. They are not accessible at run-time without the key."

4. Moskowitz — (col. 6, lines 44 - 48): "Either the user must have the extracted watermark, or the application cannot be used... In order to extract a digital watermark, the user must have a key."

5. Moskowitz — (col. 6, lines 48 - 50): "The key ... is a function of the license information for the copy of the software in question."

6. Moskowitz — (claim 4): "licensing information is selected from a group comprising an owning organization name, a personal owner name, an owner address, a license code, a software serial number, a distribution parameter..."

7. Moskowitz — (col. 6, lines 54 - 56): "The key and the license information are, in fact, interchangeable. One is merely more readable than the other."

disclose how this personal information about the user is recovered from a key). Moskowitz also provides schemes to make it difficult or effectively impossible for an attacker to remove the watermark or to break the mechanism that requires the external key.[8]

Significantly, Moskowitz teaches that *it is the authorized user who inputs his or her own personal information into the key during program installation*, and that the separate external key required to operate the program is generated by the user's action in the user's environment.[9] In other words, according to Moskowitz, the software publisher or distributor delivers the program to the authorized user *without* embedded personal information about that user. In the Moskowitz scheme, the software is sent to the authorized user containing at most a "license code". Moskowitz does not teach including personal information about the user in the "license code".[10] In summary, according to Moskowitz: any personal information about the user is gathered and input by the user, to be stored in a key which is generated when the user first launches the program after installation.

General Discussion of the Present Invention as Distinct from Moskowitz, et al.

The present invention, however, has a fundamentally different approach to protecting computer software, by *associating personal information about the customer (authorized user) within the software itself at the time of the build by the software publisher (or*

---

8. Moskowitz — *e.g.*, (col. 7, lines 22 - 29): "A second method according to the present invention is to randomly re-organize program memory structure to prevent attempts at memory capture or object code analysis. The object of this method is to make it extremely difficult to perform memory capture-based analysis of an executable computer program. This analysis is the basis for a method of attack to defeat the system envisioned by the present invention."

9. Moskowitz — (col. 6, lines 22 - 31): "The application {*i.e.*, the program} can then operate as follows: ... when it is run for the first time, after installation, it asks the user for personalization information which includes the license code... Once it has the license code, it can then generate the proper decoding key to access the essential code resources."

10. Moskowitz offers no definition of "license code" nor specifies what a "license code" constitutes. In claim 4, however, Moskowitz does enumerate a "license code" as an item *distinct* from information about the authorized user: "licensing information is selected from a group comprising an owning organization name, a personal owner name, an owner address, a license code, ..."

distributor), prior to delivery of the software to the customer, and prior to customer setup.[11] The Applicant asserts that doing so will discourage the authorized user from distributing unauthorized copies, because unauthorized copies will carry personal information about him or her. According to the present invention, this is the *sole* mechanism for deterring unauthorized distribution.[12] A goal of the present invention is *to avoid* usage and copy restrictions on software, because of the burden they place on users and the negative marketing impact that results from usage and copy restrictions. The present invention introduces no separate external keys nor places usage restriction of any kind on the computer program — copies of programs operate normally in any compatible computer environment.[13] According to the present invention, the user need not enter any keys, perform any validation procedures, or apply any other kind of special activation to attain full use of the software.

---

11. For example, in the present application (page 39 lines 16 - 23): "The present invention provides for software that already contains embedded pre-existing personal information related to the authorized user prior to delivery to the authorized user, such that the authorized user has a personal incentive to protect the software from indiscriminate unauthorized copying and distribution.

"It is an object of the present invention to provide a means for personalizing software in a way that pre-existing personal information associated with the authorized user is already present in the software at the time of delivery to the user, prior to any setup required to install the software in the user's computer."

Also see Figure 3, where in step **312** personal information is embedded in the software prior to delivery to the customer in step **316**.

12. For example, in the present application (page 40 lines 7 - 15): "It is also an object of the present invention that the incorporation of a personalization into the software application produce no side-effects that could adversely affect the operation of the software application.

"It is additionally an object of the present invention that the protection afforded by the personalization neither be associated with any usage restrictions nor activate any usage restrictions, so that deliverable published software protected solely by the personalization be operational in substantially identical functional form at all times, all places, and for unrestricted use."

13. For example, in the present application (page 40 lines 20 - 24): "...it is an object of the present invention that the inclusion of a personalization itself does not interfere with any normal operation of the deliverable published software containing the personalization, and that the personalization itself not be used in conjunction with any usage control."

Because the present invention relies solely and entirely on the presence of a personalization in the software to discourage unauthorized distribution, the present invention places heavy emphasis on embedding the personalization in a secure manner within the software, to prevent users from disabling the personalization, such as by substituting false or illegible personal information.[14] In order to meet this goal, the present invention requires that the personal information about the authorized user be embedded into the software prior to delivery to the authorized user, and in a way that it will be difficult or impossible for the user to remove or alter the personalization, such as by means of strong cryptographic techniques.

It is the intention of the Applicant, therefore, that the present invention be distinguished as much as possible from prior art such as Moskowitz.

As previously noted, according to the present invention, a personalization of the software containing personal information about the authorized user is embedded directly in the software, not in a separate key as with Moskowitz. *The personal information is furthermore embedded by the publisher (or distributor) before sending the software to the user, whereas with Moskowitz personal information is inserted by the user after receiving the software.*[15] With the present invention, the personalization can therefore be better protected against tampering by secure cryptographic techniques.[16]

---

14. For example, in the present application (page 39 line 24 - page 40 line 2): "...it is an object of the present invention to make it unfeasible for an attacker to alter or remove the personalization from the software, and to render software without such personalization incompatible with authorized copies of the software that have a valid personalization."

15. Please see note 9.

16. For example, in the present application (page 42 lines 16 - 22): "...personalization of software during the build process allows the use of cryptographic keys that offer improved authentication and security. In contrast to prior-art personalization applied as a side issue by the user during setup, where keys are necessarily short (and therefore weak), personalized cryptographic keys automatically integrated into the software during build according to the present invention can be as strong as

There are other distinctions as well. With the Moskowitz scheme, for example, a customer can give out copies of the program before installing it and putting a personalization in the key. Recipients of the copies can therefore install the program on their own computers and can personalize the keys however they wish. This cannot be done with the present invention, because the program is already non-changeably personalized when received by the customer.

According to the present invention, additional protection against tampering with the personalization can be provided in the environment of the software's user community by having the software include the cryptographically-secure personalization in output files and by having the software require a valid personalization in an input file before that file is accepted for input.[17] This is a novel feature of the present invention which does not appear in Moskowitz.

Moreover, in order to create a deterrent to unauthorized distribution of the software, the present invention expressly stipulates that the personal information of the personalization be displayed prominently by the software and its environment in a manner which Moskowitz fails to disclose.[18] The objective is that, by making the authorized user aware that his or her name and related personal information will be readily visible, there will be a disincentive for that user to give away copies of the software to others. In contrast, Moskowitz discloses no such thing, and fails to disclose how personal information (if any) contained in the external

---

desired. This is very important, as it is the only way of embedding true cryptographic-level security into a software protection system."

17. For details regarding "external validation" according to the present invention, please see the present application, page 70 line 16 through page 74 line 4, and also Figure 12.

18. For example, in the present application, page 68 lines 13 - 20: "...the software application is capable of displaying all or part of the personal information within the personalization, such as upon request by the user (in a 'help window' or 'about window') or automatically when the software application is started (in a 'splash window'), during regular execution of the software application (such as by putting the user's name in the 'title bar' or 'banner' of the software application's main window), or even interactively (such as by referring to the user by name when the software application makes a routine notification)."

key, is to be extracted and viewed. Instead, Moskowitz relies on the key to protect the software.

The Applicant respectfully submits that:

- the Moskowitz disclosure, which bases a separate external key (necessary to execute a program) partially on optional personal information is distinct from and does not anticipate the claims of the present application which are directed to the embedding of required personalized information directly in the program itself;
- the Moskowitz scheme imposes mandatory usage restrictions on the program (the need to have a special key), and does not anticipate the claims of the present application which expressly exclude such usage restrictions;
- the Moskowitz disclosure, which teaches the input of personal information by the authorized user during program installation, does not anticipate the claims of the present application which are directed to the embedding of personal information about the authorized user into the software by the software publisher or distributor prior to the delivery of the software to the authorized user; and
- the Moskowitz disclosure, which merely implies the optional display of personal information while being input by the authorized user during program installation, does not anticipate the claims of the present application which are explicitly directed to the prominent display of the personal information, such as during setup, launch, routine use of the software, viewing of software properties, and at other similar times.

Specific Office Action §102(b) Claim Rejections in Detail

Regarding the §102(b) rejection of independent claim 1: In the Office Action, page 4, it is stated that "Moskowitz et al discloses an arrangement for software protection comprising a personalization, said personalization incorporated into the information stream by the software publisher and containing pre-existing personal information fundamentally related to the customer (see column 6 lines 9-37 where the information stream is the computer code)."

The above-referenced rejection of claim 1 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, from which it can be seen that Moskowitz specifies that personal information related to the customer is *not* incorporated into the information stream by the software publisher, but *only* by the user (the customer) after installation (after receiving the program from the software publisher):

- "1) when it {the application, the computer program} is run for the first time, after installation, it asks the user for personalization information..."

While continuing to respectfully traverse the above-referenced §102(b) rejection of claim 1, in order to expedite the processing of the present application, the Applicant has elected to amend claim 1 to contain additional limitations disclosed in the present application, and which are not disclosed in the prior art, and which further distinguish claim 1 from Moskowitz, et al. The additional limitations recited in the above amendment are supported by the present application as previously noted.[19] No new material has been entered.

The Applicant therefore respectfully submits that the current response serves to remove the rejection of claim 1.

---

19. Please see note 11 for details of support in the present application for the current amendment to claim 1.

Regarding the §102(b) rejection of dependent claim 2: In the Office Action, page 4, it is stated that "Moskowitz et al discloses the deliverable software is intended to execute on a plurality of computers, and wherein said personalization is not fundamentally related to any specific computer of the plurality (see column 6 lines 9-37)."

The above-referenced rejection of claim 2 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and makes no reference to a plurality of computers, nor to any specific computer of a plurality. In fact, the entirety of the cited Moskowitz patent fails to disclose anything pertaining to a "plurality of computers" (nor to a "multiplicity of computers", "many computers", "more than one computer", etc.). Furthermore, the cited passage from Moskowitz implies that the user is installing the application program on a single computer belonging to the user.

The Applicant furthermore notes that claim 2 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 2.

Regarding the §102(b) rejection of dependent claim 3: In the Office Action, page 4, it is stated that "Moskowitz et al discloses the deliverable published software is intended to execute on a plurality of computers, each of the plurality of computers having a configuration, and wherein said personalization is not fundamentally related to any specific configuration (see column 6 lines 22-31)."

The above-referenced rejection of claim 3 is respectfully traversed. As noted above, neither the cited excerpt from Moskowitz (which appears in this response on page 34) nor the Moskowitz patent in its entirety make any reference to a plurality of computers.

Moreover, the cited excerpt expressly states that personalization information *can* be fundamentally related to a specific configuration:

- "...it {the application, the computer program} asks the user for personalization information, which includes the license code. This can include a particular computer configuration;"

The Applicant furthermore notes that claim 3 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 3.

Regarding the §102(b) rejection of dependent claim 4: The Applicant accepts the Examiner's observation on page 5 of the Office Action, that "...it is inherent of Java to execute substantially identical on all computers." However, the Applicant notes that claim 4 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 4.

Regarding the §102(b) rejection of dependent claim 5: The Applicant notes that through a typographical error, a key word was unintentionally and inadvertently omitted from the original text of claim 5. The above amendment corrects the typographical error by restoring the omitted key word.

With the foregoing amendment, dependent claim 5 is clearly distinct from Moskowitz, because Moskowitz discloses a method that *is* associated with and *does activate* a usage restriction on the deliverable published software — the software according

to Moskowitz is usage-restricted from being operated if the user does not have the key[20], and the personalization (if any) is contained in the key.[21]

The Applicant therefore believes the current amendment to claim 5 serves to remove the above rejection. The Applicant furthermore notes that claim 5 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 5.

Regarding the §102(b) rejection of dependent claim 6: In the Office Action, page 5, it is stated that "Moskowitz et al discloses the personalization does not have a fixed address within the information stream (see column 6 lines 9-37).

The above-referenced rejection of claim 6 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and makes no reference to the address of a personalization, nor to the address of any portion of an information stream. In fact, the Moskowitz patent in its entirety fails to disclose anything pertaining to the address of a personalization. Moskowitz discusses the issue of addresses in computer memory of executable code, but nothing pertaining to the address of elements within information streams.

The Applicant furthermore notes that claim 6 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1.

---

20. Moskowitz — (col. 6, lines 44 - 48): "Either the user must have the extracted watermark, or the application cannot be used... In order to extract a digital watermark, the user must have a key."

21. Moskowitz — (col. 6, lines 48 - 50): "The key ... is a function of the license information for the copy of the software in question"; (claim 4): "licensing information is selected from a group comprising an owning organization name, a personal owner name, an owner address...{*i.e.*, personal information, a personalization}"; (col. 6, lines 54 - 56): "The key and the license information are, in fact, interchangeable. One is merely more readable than the other."

Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 6.

Regarding the §102(b) rejection of dependent claim 7: In the Office Action, page 5, it is stated that "Moskowitz et al discloses the personalization does not have a fixed extent with the information stream (see column 6 lines 9-37).

The above-referenced rejection of claim 7 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and makes no reference to the extent of a personalization, nor to the extent (or "size") of any portion of an information stream. In fact, the Moskowitz patent in its entirety fails to disclose anything pertaining to the extent (or "size") of a personalization, or to the extent of elements within information streams.

The Applicant furthermore notes that claim 7 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 7.

Regarding the §102(b) rejection of dependent claim 10: The Applicant accepts the Examiner's observation that "Moskowitz et al discloses the information stream contains at least one executable module operative to displaying at least part of said personalization ... where it is inherent that the information will be displayed when being entered..."

However, because the present invention provides for display of at least part of the personalization without requiring any entry thereof[22], in contrast to entry by the user as

22. For example, in the present application, page 68 lines 13 - 21: "...the software application is capable of displaying all or part of the personal information within the personalization, such as ... automatically ... in a 'splash window' ... the user's name in the 'title bar' or 'banner' ... referring to the user by name when the software application makes a routine notification... in a 'properties' page..." etc.

disclosed in Moskowitz[23], the Applicant has elected to cancel claim 10 and to provide new dependent claims 31, 32, and 33 to replace present claim 10 and to include additional limitations as disclosed in the present application which distinguish new dependent claims 31, 32, and 33 from the incidental entry-accompanying display mode of Moskowitz. Support for new dependent claims 31, 32, and 33 is found in the present application as noted above.[24] No new material has been entered.

The Applicant furthermore notes that new claims 31, 32, and 33 depend from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to render new dependent claims 31, 32, and 33 free of the basis of rejection applied to canceled claim 10.

Regarding the §102(b) rejection of dependent claim 11: In the Office Action, page 5, it is stated that "Moskowitz et al discloses the information stream contains at least one executable module, and wherein said personalization is contained within said at least one executable module (see column 6 lines 9-37)."

The above-referenced rejection of claim 11 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and makes no reference to an executable module (or executable code), neither in the information stream nor otherwise. Furthermore, Moskowitz discloses that a personalization (if any) is contained within an

---

23. Moskowitz — (col. 6, lines 22 - 24): "The application {*i.e.*, the program} can then operate as follows: ... when it is run for the first time, after installation, it asks the user for personalization ..."

24. Please see note 22 above.

external key[25], and a key is considered throughout the art to be a piece of data, not executable code.

The Applicant furthermore notes that claim 11 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 11.

Regarding the §102(b) rejection of dependent claim 12: The Applicant accepts, with an adjustment, the Examiner's observation on pages 5 and 6 of the Office Action, that "Moskowitz et al discloses a personalization validation module operative to validating a personalization ... where extracting the watermark is the validation and the key is part of the personalization" — the adjustment being that, according to Moskowitz, the key optionally *contains* the personalization, rather than is "part of" the personalization.[26]

However, the Applicant notes that claim 12 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 12.

Regarding the §102(b) rejection of dependent claim 13: The Applicant accepts the Examiner's observation on page 6 of the Office Action, that "Moskowitz et al discloses the

---

25. Moskowitz — (col. 6, lines 44 - 48): "Either the user must have the extracted watermark, or the application cannot be used... In order to extract a digital watermark, the user must have a key"; (col. 6, lines 48 - 50): "The key ... is a function of the license information for the copy of the software in question"; (claim 4): "licensing information is selected from a group comprising an owning organization name, a personal owner name, an owner address...{*i.e.*, personal information, a personalization}"; (col. 6, lines 54 - 56): "The key and the license information are, in fact, interchangeable. One is merely more readable than the other."

26. Please see note 25.

personalization validation module is further operative to validate an output file ... where the software is an output file and the watermark is used to validate it."

However, the Applicant notes that claim 13 depends from claim 1 (through claim 12), and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 13.

Regarding the §102(b) rejection of dependent claim 14: The Applicant accepts, subject to a clarification, the Examiner's observation on page 6 of the Office Action, that "Moskowitz et al discloses the information stream contains at least one executable module, and wherein said personalization verification module is further operative to validating said at least one executable module" — the clarification being that, according to Moskowitz, the executable module is the software.

However, the Applicant notes that claim 14 depends from claim 1 (through claim 12), and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 14.

Regarding the §102(b) rejection of dependent claim 15: The Applicant accepts, subject to a clarification, the Examiner's observation on page 6 of the Office Action, that "Moskowitz et al discloses the personalization validation module is further operative, upon not detecting a valid personalization, to initiate an action included in the group containing: (a) program termination; (b) operating the software in a demonstration mode; and (c) operating the software in a restricted mode" — the clarification being that, according to Moskowitz, not being given a valid key is construed as "not detecting a valid

personalization", and not allowing the software to operate at all is construed as "program termination".

However, the Applicant notes that claim 15 depends from claim 1 (through claim 12), and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 15.

Regarding the §102(b) rejection of dependent claim 17: The Applicant accepts the Examiner's observation on page 6 of the Office Action, that "Moskowitz et al discloses at least part of the deliverable published software is written in the Java language."

However, the Applicant notes that claim 17 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 17.

Regarding the §102(b) rejection of dependent claim 21: In the Office Action, page 7, it is stated that "Moskowitz et al discloses the personalization is in an encrypted form within the information stream, and wherein said personalization validation module is further operative to decrypting said encrypted form (see column 6 lines 9-37)."

The above-referenced rejection of claim 21 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and makes no mention of encrypting the personal information (a personalization), nor decrypting thereof. In fact, the Moskowitz patent in its entirety fails to disclose decrypting encrypted personal information.

The Applicant furthermore notes that claim 21 depends from claim 1 (through claim 12), and that the Applicant believes the current response serves to remove the rejection of

claim 1. Consequently, the Applicant respectfully submits that in any event, the current response also serves to remove the rejection of claim 21.

Regarding the §102(b) rejection of dependent claim 23: The Applicant accepts, with a clarification, the Examiner's observation on page 7 of the Office Action, that "Moskowitz et al discloses the information stream contains at least one executable module operative to writing an output file containing information derived from said personalization" — the clarification being that, according to Moskowitz, the output file is a key, which can be based on personal information.[27]

However, the present invention provides for validation of the personalization in an output file (when the output file is treated as an input file for reading the data therein), and this validation of the personalization is separate from any validation of the output file as a whole.[28] In contrast, the key of Moskowitz may be validated, but the personal information (if any) contained in the key cannot be separately validated. Applicant has elected to amend claim 23 to emphasize this distinction compared to Moskowitz. The additional limitations recited in the above amendment are supported by the present application as just noted.

The Applicant furthermore notes that claim 23 depends from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the rejection of claim 23.

---

27. See note 21, for example.

28. In the present application, for example, Figure 12 and the discussion thereof on page 70 - 74. In particular, page 70 line 24 - page 71 line 5: "...a software application **1202** containing a personalization **1204** writes an output file **1208** containing a copy of personalization **1204** in each output operation **1206**. Subsequently, when output file **1208** is read via an input operation **1210** by a different instance of the software application **1212** ... personalization **1204** is read ... and can be validated by the personalization validation module..."

Regarding the §102(b) rejection of independent claim 24: The Applicant accepts the Examiner's observation on page 7 of the Office Action that "Moskowitz et al discloses (a) obtaining pre-existing personal information fundamentally related to the customer; (b) producing, from said pre-existing personal information fundamentally related to the customer, a personal information module; and (c) producing an executable module deriving at least in part from said personal information module and incorporating said pre-existing personal information fundamentally related to the customer (see column 6 lines 9-37)."

However, Applicant notes that personal information according to Moskowitz does not serve to protect the software as stipulated by the preamble of claim 24. In contrast, it is a central point of the present invention that the software already be protected by a personalization when received by the customer. Therefore, the Applicant has amended claim 24 to contain limitations that require the personalization to be incorporated into the published software prior to delivery to the customer and prior to receipt by the customer (the authorized user) in order to effect the desired protection. These limitations are supported by the present application, as previously discussed.[29] In addition, the Applicant has also amended claims 24 - 26 for improved clarity. No new material has been entered.

The Applicant therefore respectfully submits that the current response serves to remove the rejection of claim 24.

Regarding the §102(b) rejection of independent claim 28: In the Office Action, pages 7 - 8, it is stated that "Moskowitz et al discloses (a) a personal information collector for collecting pre-existing personal information fundamentally related to the customer; (b) a personalization compiler, for producing, from said pre-existing personal information fundamentally related to the customer, a personalization module; and (c) an executable

29. Please see note 11.

module builder, for producing deliverable published software containing said pre-existing personal information fundamentally related to the customer and derived at least in part from said personalization module (see column 6 lines 9-37)."

The above-referenced rejection of claim 28 is respectfully traversed. The cited excerpt from Moskowitz appears in this response on page 31, and clearly indicates that, according to Moskowitz, *the software has already been installed* by the user and modified by the user prior to the collecting of personal information, and prior to the action of the executable module builder.[30] Claim 28, however, stipulates that the output of the executable module builder is "deliverable published software" — and this limitation was put into claim 28 to convey the condition that the software is ready for the customer, but *has not yet been installed* by the customer.[31] Thus, Moskowitz fails to disclose the precise conditions recited in claim 28.

While continuing to respectfully traverse the above-referenced §102(b) rejection of claim 28, in order to expedite the processing of the present application, the Applicant has elected to amend claim 28 to contain an additional limitation disclosed in the present application, which is not disclosed in the prior art, and which further distinguishes claim 28 from Moskowitz.

In addition, the Applicant has elected to add new claims 29 and 30, depending from claim 28, which incorporate further limitations to distinguish the present invention from Moskowitz. The additional limitations recited in the above amendment and new claims relate to the gathering of personal information remotely over a communications channel. In

---

30. Moskowitz (column 6 lines 23 - 24): "...when it is run for the first time, *after installation*, it asks the user for personalization information..." (emphasis supplied)

31. Present application (page 31 lines 12 - 14): "deliverable published software — any published software in a form ready for installation or use by a user, *prior to setup, installation, or modification* by the user." (emphasis supplied)

Moskowitz, personal information about the user is obtained directly from the user by an application running on the user's computer. As disclosed in the present application, however, the present invention gathers information from the user remotely over a communications channel. Thus, the above amendment to claim 28 is supported by the present application[32], as are new dependent claims 29 and 30.[33] No new material has been entered.

The Applicant therefore respectfully submits that the current response serves to remove the rejection of claim 28.

§103 Rejections

The Examiner has rejected claims 8-9, 16, 18 - 20, 22, and 25 - 27 under 35 U.S.C. §103(a) as being unpatentable over Moskowitz et al. as applied to claims 1 and 24, in view of other cited prior art, including Menzes, et al., and Somerer.

The Applicant notes that claims 8-9, 16, 18 - 20, and 22 depend from claim 1, and that the Applicant believes the current response serves to remove the rejection of claim 1. Consequently, the Applicant respectfully submits that the current response also serves to remove the §103 rejection of claims 8-9, 16, 18 - 20, and 22.

The Applicant further notes that claims 25 - 27 depend from claim 24, and that the Applicant believes the current response serves to remove the rejection of claim 24.

---

32. Present application: Figure 14 shows a remote communications channel **1408** between the customer and personal information collector **1414** for use with a system **1402** for protecting software ordered by a customer (the subject of claim 28); (page 78 lines 15-18): "Figure 14 conceptually illustrates a system **1402** for personalizing deliverable published software from a software publisher **1404** to a customer **1406** according to the present invention. Software publisher **1404** interacts with customer **1406** through a channel **1408...**"

33. Present application — (page 78 lines 17-18): "... a channel **1408**, non-limiting examples of which include networks such as the Internet."

Consequently, the Applicant respectfully submits that the current response also serves to remove the §103 rejection of claims 25 - 27.

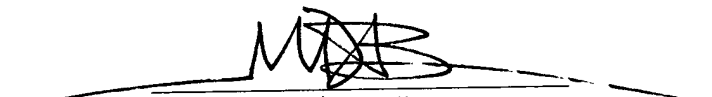
Summary

The Examiner's comments have been given careful and thorough consideration in the above amendments to the application and remarks.

The Applicant believes that the abstract of the application is now of proper length, and that claims 1-9 and 11-33 overcome the rejections detailed in the Office Action, and meet the standards as specified in 35 U.S.C. §102, §103, and §112.

In view of the above amendments and remarks it is respectfully submitted that claims 1-9 and 11-33 are in condition for allowance. Notice of allowance is therefore respectfully and earnestly solicited.

Respectfully submitted,



Moshe Brody, Applicant

Date: January 3, 2005

Appendix: Cited References to Moskowitz, et al.

For the Examiner's convenience in making reference to the above-discussed differences at the detailed level pertaining to the claims in question, herein follow the specific passages of Moskowitz et al. as cited in the Office Action:

- ***Moskowitz — col. 2 lines 45 - 60:***

  "It is a further goal of the present invention to establish methods of copyright protection that can be combined with such schemes as software metering, network distribution of code and specialized protection of software that is designed to work over a network, such as that proposed by Sun Microsystems in their HotJava browser and Java programming language, and manipulation of application code in proposed distribution of documents that can be exchanged with resources or the look and feel of the document being preserved over a network. Such systems are currently being offered by companies including Adobe, with their Acrobat software. This latter goal is accomplished primarily by means of the watermarking of font, or typeface, resources included in applications or documents, which determine how a bitmap representation of the document is ultimately drawn on a presentation device."

- ***Moskowitz — col. 6 lines 9 - 37***

  "The assembly utility can be supplied with a key generated from a license code generated for the license in question. Alternatively, the key, possibly random, can be stored as a data resource and encrypted with a derivative of the license code. Given the key, it encodes one or several essential resources into one or several data resources. Exactly which code resources are encoded into which data resources may be determined in a random or pseudo random manner. Note

further that the application contains a code resource which performs the function of decoding an encoded code resource from a data resource. The application must also contain a data resource which specifies in which data resource a particular code resource is encoded. This data resource is created and added at assembly time by the assembly utility. The application can then operate as follows:

"1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;

"2) it stores this information in a personalization data resource;

"3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources.

"Note that the application can be copied in an uninhibited manner, but must contain the license code issued to the licensed owner, to access its essential code resources. The goal of the invention, copyright protection of computer code and establishment of responsibility for copies, is thus accomplished."

- ***Moskowitz — col. 6 lines 9 - 67***

"The assembly utility can be supplied with a key generated from a license code generated for the license in question. Alternatively, the key, possibly random, can be stored as a data resource and encrypted with a derivative of the license code. Given the key, it encodes one or several essential resources into one or several data resources. Exactly which code resources are encoded into which data resources may be determined in a random or pseudo random manner. Note further that the application contains a code resource which performs the function

of decoding an encoded code resource from a data resource. The application must also contain a data resource which specifies in which data resource a particular code resource is encoded. This data resource is created and added at assembly time by the assembly utility. The application can then operate as follows:

"1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;

"2) it stores this information in a personalization data resource;

"3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources.

"Note that the application can be copied in an uninhibited manner, but must contain the license code issued to the licensed owner, to access its essential code resources. The goal of the invention, copyright protection of computer code and establishment of responsibility for copies, is thus accomplished.

"This invention represents a significant improvement over prior art because of the inherent difference in use of purely informational watermarks versus watermarks which contain executable object code. If the executable object code in a watermark is essential to an application which accesses the data which contains the watermark, this creates an all-or-none situation. Either the user must have the extracted watermark, or the application cannot be used, and hence the user cannot gain full access to the presentation of the information in the watermark bearing data. In order to extract a digital watermark, the user must have a key. The key, in turn, is a function of the license information for the copy of the software in question. The key is fixed prior to final assembly of the

application files, and so cannot be changed at the option of the user. That, in turn, means the license information in the software copy must remain fixed, so that the correct key is available to the software. The key and the license information are, in fact, interchangeable. One is merely more readable than the other. In U.S. Pat. No. 5,613,004, the 'Steganographic Method and Device, patent', the possibility of randomization erasure attacks on digital watermarks was discussed. Simply, it is always possible to erase a digital watermark, depending on how much damage you are willing to do to the watermark-bearing content stream. The present invention has the significant advantage that you must have the watermark to be able to use the code it contains. If you erase the watermark you have lost a key piece of the functionality of the application, or even the means to access the data which bear the watermark."

- ***Moskowitz — col. 6 lines 22 - 31***

  "1) when it is run for the first time, after installation, it asks the user for personalization information, which includes the license code. This can include a particular computer configuration;

  "2) it stores this information in a personalization data resource;

  "3) Once it has the license code, it can then generate the proper decoding key to access the essential code resources."

- ***Moskowitz — col. 6 lines 38 - 67***

  "This invention represents a significant improvement over prior art because of the inherent difference in use of purely informational watermarks versus watermarks which contain executable object code. If the executable object code in a watermark is essential to an application which accesses the data which contains the watermark, this creates an all-or-none situation. Either the user

must have the extracted watermark, or the application cannot be used, and hence the user cannot gain full access to the presentation of the information in the watermark bearing data. In order to extract a digital watermark, the user must have a key. The key, in turn, is a function of the license information for the copy of the software in question. The key is fixed prior to final assembly of the application files, and so cannot be changed at the option of the user. That, in turn, means the license information in the software copy must remain fixed, so that the correct key is available to the software. The key and the license information are, in fact, interchangeable. One is merely more readable than the other. In U.S. Pat. No. 5,613,004, the 'Steganographic Method and Device, patent', the possibility of randomization erasure attacks on digital watermarks was discussed. Simply, it is always possible to erase a digital watermark, depending on how much damage you are willing to do to the watermark-bearing content stream. The present invention has the significant advantage that you must have the watermark to be able to use the code it contains. If you erase the watermark you have lost a key piece of the functionality of the application, or even the means to access the data which bear the watermark."